DEPARTMENT OF THE ARMY
UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
UNIT 29351
APO AE 09014-9351

AEAGD-ELSD

6 May 2005

MEMORANDUM FOR All G4 Personnel

SUBJECT: G4 Policy - Computer User Responsibilities

1. References:

a. AR 25-1, Army Knowledge Management and Information Technology Mgmt, 30 June 2004.
b. Army in Europe Supplement 1 to AR 25-1, 21 April 2005.
c. AR 25-2, Information Assurance, 14 November 2003.
d. Army in Europe Supplement 1 to AR 25-2, 25 December 2004.

2. Reference publications contain directives concerning computer user responsibilities. However, I want to be sure that all G4 Personnel are fully aware of their responsibility to protect the information processed by government computers, use government computers only for official purposes, and to refrain from any action which may be harmful to government computer systems or limit their effectiveness. The guiding principle here is that government information and government computers/networks are "**For Official Use Only**".

3. Protection of government information is your responsibility. In particular, I want to emphasize the importance of E-Mail Security. Ensure that sensitive unclassified information sent via **Unclassified E-Mail** is **encrypted**, and that **classified E-Mail is sent only via the SIPRNET**. Computer users shall not auto forward Official E-Mail to Non-Official E-Mail services such as Hot Mail or Yahoo. Discipline and common sense procedural security are crucial when using USB Memory Sticks. Ensure you use only government provided memory sticks, and are labeled either UNCLASSIFIED or SECRET.

4. Every computer user must understand the computer on his/her desk is only for the purpose of supporting his efforts to accomplish his assigned duties. Use of a government computer for personal purposes is prohibited except as provided in AR 25-1, paragraph 6-1,d,(6)e. Computer users will not install software of any kind on their government computer without the approval of the G4 Information Management Officer. **Unofficial E-Mail messages containing attachments will not be sent or forwarded.** Above all, quoting AR 25-2, computer users will not "***Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications.***"

for Sarah W. Simmons
LARRY C. NEWMAN
Brigadier General, GS
Deputy Chief of Staff, G4

DEPARTMENT OF THE ARMY
UNITED STATES ARMY, EUROPE, AND SEVENTH ARMY
UNIT 29351
APO AE 09014-9351

AEAGD

5 May 2005

MEMORANDUM FOR All G4 Personnel

SUBJECT: G4 Policy - Computer User Responsibilities

1. References:
   a. AR 25-1, Army Knowledge Management and Information Technology Mgmt, 30 June 04.
   b. Army in Europe Supplement 1 to AR 25-1, 21 April 2005.
   c. AR 25-2, Information Assurance, 14 November 2003.
   d. Army in Europe Supplement 1 to AR 25-2, 25 December 2004.

2. Reference publications contain directives concerning computer user responsibilities. However, I want to be sure that all G4 Personnel are fully aware of their responsibility to protect the information processed by government computers, use government computers only for official purposes, and to refrain from any action which may be harmful to government computer systems or limit their effectiveness. The guiding principle here is that government information and government computers/networks are "**For Official Use Only**".

3. Protection of government information is your responsibility. In particular, I want to emphasize the importance of E-Mail Security. Ensure that sensitive unclassified information sent via Unclassified E-Mail is **encrypted**, and that **classified E-Mail is sent only via the SIPRNET**. Computer users shall not auto forward Official E-Mail to Non-Official E-Mail services such as Hot Mail or Yahoo. Discipline and common sense procedural security are crucial when using USB Memory Sticks. Ensure that you use only government provided memory sticks, and that they are labeled either UNCLASSIFIED or SECRET.

4. Every Computer user must understand that the computer on his desk is there only for the purpose of supporting his efforts to accomplish his assigned duties. Use of a government computer for personal purposes is prohibited except as provided in AR 25-1, paragraph 6-1,d,(6)e. Computer users will not install software of any kind on their government computer without the approval of the G4 Information Management Officer. **Unofficial E-Mail messages containing attachments will not be sent or forwarded.** Above all, quoting AR 25-2, computer users will not "***Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications***."

LARRY C. NEWMAN
Brigadier General, GS
Deputy Chief of Staff, G4

Army in Europe
Supplement 1 to AR 25-2

25 December 2004

Information Management: Management of Subdisciplines

Army Information Assurance

Paragraph 4-6, Controls. Add subparagraphs q and r as follows:

q. Software may be loaded on GCs only with the approval of the DAA and must be coordinated with the IAM or IASO.

r. Prohibited software in the Army in Europe includes the following:

(1) Games other than Army-sanctioned simulations and games preloaded (factory-installed) on the GC. (*America's Army* is not an Army-sanctioned simulation.)

(2) Hacker tools.

(3) Malicious logic software.

(4) Streaming audio and video, unless authorized by the USAREUR G6 in coordination with the 5th Sig Cmd G3 for official purposes.

(5) Unauthorized Freeware and Shareware.

(6) Unauthorized keystroke-monitoring tools.

(7) Unauthorized network-monitoring tools.

(8) Unauthorized peer-to-peer file-sharing software (for example, digital video disks (DVDs), MP3 music, music CD-ROMs, and video software).

(9) Unlicensed commercial (pirated) software.

(10) Firewalls not managed by the SA.

(11) Web page-altering software (for example, Bearshare, Cydoor, Gator, Limewire, TopText).

Paragraph 4-16, Protection Requirements. Add subparagraph h as follows:

h. All removable computer-system media (for example, CD-ROMs, DVDs, floppy disks, tapes, universal serial bus (USB) drives (memory sticks, pen drives, thumb drives)) must be Government-owned and properly marked, controlled, stored, transported, and destroyed based on classification or sensitivity and need-to-know. All removable media will be scanned for viruses before use on Government systems. In the Army in Europe, the use of personally owned media on the LandWarNet (Unclas) or LandWarNet (Class) is prohibited.

Paragraph 4-20g, Internet, Intranet, Extranet, and WWW Security. Add subparagraph (17) as follows:

(17) The AKO Internet chat tool is the only chat tool authorized for use on the Army in Europe LandWarNet (Unclas).

Paragraph 4-30a, Employee-Owned Information Systems. Add the following:

EOIs (including memory sticks, media, and PEDs) are prohibited on Army in Europe networks and will not be used to process classified or unclassified sensitive information.

Army Regulation 25-2

14 November 2003

Effective date: 14 November 2003

UNCLASSIFIED

Information Management: Management of Subdisciplines

Information Assurance

3-3. Information Assurance support personnel

c. General users. Users are the foundation of the DiD strategy and their actions affect the most vulnerable portion of the AEI. Users must have a favorable background investigation or hold a security clearance or access approvals commensurate with the level of information processed or available on the system.

(1) User responsibilities.

(a) Comply with the guidelines established under the DOD 5500.7 when making personal use of government-owned ISs.

(b) Participate in annual IA training inclusive of threat identification, physical security, acceptable use policies, malicious content and logic, and non-standard threats such as social engineering.

(c) Mark and safeguard files, output products, and storage media per the classification level and disseminate them only to individuals authorized to receive them and with a valid need to know.

(d) Protect ISs and IS peripherals located in their respective areas in accordance with physical security and data protection requirements.

(e) Practice safe network and Internet operating principles and take no actions that threaten the integrity of the system or network.

(f) Safeguard and report any unexpected or unrecognizable output products.

(g) Report the receipt of any media (for example, CD-ROM, floppy disk) received to the IAM or SA, as appropriate, for authorization to use.

(h) Use anti-virus (AV) products on all files, attachments, and media before opening or introducing them into the IS.

(i) Report all known or suspected security incidents, spam, chain letters, and violations of acceptable use to the SA, IAM, or IASO.

(j) Immediately report suspicious, erratic, or anomalous IS operations, and missing or added files, services, or programs to the SA in accordance with local policy and cease operations on the affected IS.

(k) Comply with password or pass-phrase policy directives and protect passwords from disclosure.

(l) Invoke automatic password-protected screen locks on the workstation after not more than 10 minutes of non-use or inactivity.

(m) Logoff ISs at the end of each workday.

(n) Access only that data, control information, software, hardware, and firmware for which they are authorized access and have a need to know, and assume only authorized roles and privileges.

(o) Users authorized government-provided IA products (for example, AV or personal firewalls) should be encouraged to install and update these products on their personal systems and may be required to do so as directed by the DAA for any approved remote access.

(2) Prohibited activities. The following activities are specifically prohibited and users will not —

(a) Use ISs for personal commercial gain or illegal activities.

(b) Use ISs in any manner that interferes with official duties, undermines readiness, reflects adversely on the Army, or violates standards of ethical conduct.

(c) Intentionally send, store, or propagate sexually explicit, threatening, harassing, political, or unofficial public activity (that is, spam) communications. (LE/CI investigators, attorneys, or other official activities, operating in their official capacities only, may be exempted from this requirement.)

(d) Participate in on-line gambling or other activities inconsistent with public service.

(e) Participate in, install, configure, or use ISs in any commercial or personal DCE (for example, SETI, human genome research).

(f) Release, disclose, or alter information without the consent of the data owner, the original classification authority (OCA) as defined by AR 380-5 , the individual's supervisory chain of command, Freedom of Information Act (FOIA) official, Public Affairs Office, or disclosure officer's approval.

(g) Attempt to strain, test, circumvent, bypass security mechanisms, or perform network line monitoring or keystroke monitoring.

(h) Modify the system equipment or software, use it in any manner other than its intended purpose, introduce malicious software or code, or add user-configurable or unauthorized software (for example, instant messaging, peer-to-peer applications).

(i) Relocate or change IS equipment or the network connectivity of IS equipment without proper security authorization.

(j) Share personal accounts and passwords or permit the use of remote access capabilities by any individual.

(k) Disable or remove security or protective software or mechanisms and their associated logs.

4-20. Network security

f. E-mail security. E-mail systems will be used only for transmission and receipt of communications equivalent to or less than the classification level of the IS.

(1) IA personnel will —

(a) Promote security awareness.

(b) Use encryption when available or as part of the global enterprise (when implemented) to secure the sensitivity requirements of the data.

(c) Ensure the physical security of any information and the mail server.

(d) Install and configure antiviral software on e-mail servers and client workstations.

(e) Warn users to treat unusual e-mail messages the same way they treat unusual parcels — with caution.

(f) Use digital signatures to authenticate a message as needed (non-repudiation).

(g) Configure ISs to prevent opening attachments or active code directly from mail applications when available.

(2) Personnel will not share personal e-mail accounts. Commanders may allow the limited use of organizational or group e-mail accounts where operationally warranted.

(3) E-mail passwords will differ from the network password when used, until a global PKI initiative is available.

(4) Personnel will employ government owned or provided e-mail systems or devices for government communications and the use of commercial ISP or e-mail accounts for official purposes is prohibited.

(5) Auto-forwarding of official mail to non-official accounts or devices is prohibited.

(6) Permit communications to vendors or contractors to conduct official business and implement encryption and control measures appropriate for the sensitivity of the information transmitted.

(7) Personnel will scan all files for viruses before storing, transmitting, or processing information.

(8) Authorized users who are contractors, DOD direct or indirect hires, foreign nationals, or foreign representatives will have their respective affiliations displayed as part of their e-mail addresses.

Army in Europe
Supplement 1 to AR 25-1

21 April 2005

Information Management

Army Knowledge Management and Information Technology Management

Paragraph 6-2e(4), Software Control. Add the following:

Organizational IMOs, IASOs, or system administrators are responsible for centrally managing and keeping the original software media (installation CDs or diskettes, certificates of authenticity) and approval, registration, warranty, and disposition records. These records must be available for review (for example, by the judge advocate, inspector general, software companies). No software may be installed on Army in Europe networks without written approval of the organizational IMO, IASO, or system administrator. "Army in Europe networks" include local area networks (LANs), departmental local area networks, wireless-enabled portable electronic devices (PEDs), and standalone PCs. A copy of this approval must be kept with software records.

Paragraph 6-3, Network Operations (NETOPS).

j. Remote Access. The AE remote-access request forms (categories 1 and 2) will be used by personnel in Europe to request remote access to the Army in Europe LandWarNet (Unclas). (See paragraph E-5 for more information.)

(1) The category 1 form (AE Form 25-1H) will be used by DOD military personnel, DOD civilian employees, and permanently hired contractor personnel assigned to DOD agencies stationed in the European theater.

(2) The category 2 form (AE Form 25-1J) will be used by contractor personnel who are temporarily hired to accomplish specific official tasks that require remote access to the network.

(3) The forms must be completed by the requesting user, the unit IMO,

and the approving authority (either a commander in the grade of O3 (for example, an Army captain) or higher, or a GS-13 or higher supervisor).

(4) Commanders approving remote access for their personnel must provide correctly configured Government-owned information systems (GOISs) for each user. AE Form 25-1K will be used to ensure correct equipment and configuration.

(5) The COR will also complete a portion of the category 2 form to validate that the requesting user is assigned to the contract and has an official requirement to remotely connect to the network.

(6) After the form has been completed and approved, the unit IMO will use it to complete an account request with the SSB.

(7) AR 25-400-2 requires that these forms be maintained in official unit files until the account is terminated or closed by the IMO in coordination with the SSB.

(8) Employee-owned information systems (EOISs) are not authorized to be used to remotely connect to the AE LandWarNet (Unclas).

ARMY KNOWLEDGE MANAGEMENT AND INFORMATION TECHNOLOGY MANAGEMENT

d. Official uses of telecommunications and computing systems.

(1) The use of DOD and other Government telephone systems, electronic mail (e-mail), and other systems (including the Internet) are limited to the conduct of official business or other authorized uses. Commanders and supervisors at all levels will make anyone using Government telecommunications systems aware of permissible and unauthorized uses. Local policies and procedures will be promulgated, as necessary, to avoid disruptions of telecommunications systems. (Authorized use is defined in e, below.) The Joint Ethics Regulation, Section 2-301, serves as the basis for Army policy on the use of telecommunications and computing systems. Users will abide by these restrictions to prevent security compromises and disruptions to Army communications systems.

(2) All communications users must be aware of security issues, their consent to monitoring for all lawful purposes, restrictions on transmitting classified information over unsecured communications systems, prohibitions regarding release of access information such as passwords, and of the need for caution when transmitting other sensitive information. (See para 6-4q for additional information on communications monitoring.)

(3) Commanders will recover toll charges, as practical, for unofficial/unauthorized personal telephone calls placed on official telephones by personnel within their organizations. Charges may also apply to misuse of government communications through modem/other connections.

(4) Official business calls and e-mail messages are defined as those necessary in the interest of the Government (for example, calls and e-mail messages directly related to the conduct of DOD business or having an indirect impact on DOD's ability to conduct its business).

(5) Official use includes health, morale, and welfare (HMW) communications by military members and DOD employees who are deployed in remote or isolated locations for extended periods of time on official DOD business. When authorized by the theater combatant commander, the theater commander will institute local procedures to authorize HMW communications when commercial service is unavailable or so limited that it is considered unavailable. HMW calls may be made only during nonpeak, nonduty hours and should not exceed 15 minutes once per week. The commander may authorize calls that exceed this limit and frequency on an exception basis. (See para 6-4w for guidance on cellular telephones.)

(6) Guidance for telephone calls while at a temporary duty location is reflected in the Joint Travel Regulations .

e. Authorized uses of communication systems. Authorized use includes brief communications made by DOD employees while they are traveling on Government business to notify family members of transportation or schedule changes. They also include personal communications from the DOD employee's usual workplace that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments; brief Internet searches; e-mailing directions to visiting relatives). Such communications may be permitted, provided they —

(1) Do not adversely affect the performance of official duties by the employee or the employee's organization.

(2) Are of reasonable duration and frequency, and, whenever possible, are made during the employee's personal time, such as during lunch, break, and other off-duty periods).

(3) Are not used for activities related to the operation of a personal business enterprise.

(4) In the case of long distance (toll) calls, are —

(a) Charged to the employee's home phone number or other non-Government numbers (third party call).

(b) Made to a toll-free number.

(c) Charged to the called party if a non-Government number (collect call).

(d) Charged to a personal telephone card.

(e) Of a legitimate public interest (such as keeping employees at their desks rather than requiring the use of commercial systems; educating DOD employees on the use of communications systems; improving the morale of employees stationed for extended periods away from home; enhancing the professional skills of DOD employees; job-searching in response to Federal Government downsizing).

f. Prohibitions in telecommunications usage. Other prohibitions in the use of Army communications systems include the following:

(1) Use of communications systems that would adversely reflect on DOD or the Army (such as uses involving sexually explicit e-mail or access to sexually explicit Web sites, pornographic images, or virtual computer-generated or otherwise pornographic images); chain e-mail messages; unofficial advertising, soliciting, or selling via e-mail; and other uses that are incompatible with public service.

(2) Use of communications systems for unlawful activities, commercial purposes, or in support of for-profit activities, personal financial gain, personal use inconsistent with DOD policy, personal use that promotes a particular religion or faith, or uses that violate other Army policies or public laws. This may include, but is not limited to, violation of intellectual property, gambling, terrorist activities, and sexual or other forms of harassment.

(3) Political transmissions to include transmissions that advocate the election of particular candidates for public office.

(4) Both Federal law and Army policy prohibit, in general, the theft or other abuse of computing facilities. Such prohibitions apply to electronic mail services and include, but are not limited to: unauthorized entry, use, transfer, and tampering with the accounts and files of others and interference with the work of others and with other computing facilities.

(5) Army communications systems will not be used for purposes that could reasonably be expected to cause, directly or indirectly, congestion, delay, or disruption of service to any computing facilities or cause unwarranted or unsolicited interference with others' use of communications. Such uses include, but are not limited to, the use of communications systems to —

(a) Create, download, store, copy, transmit, or broadcast chain letters.

(b) "Spam" to exploit listservers or similar broadcast systems for purposes beyond their intended scope to amplify the widespread distribution of unsolicited e-mail.

(c) Send a "letter-bomb" to re-send the same e-mail message repeatedly to one or more recipients, to interfere with the recipient's use of e-mail.

(d) Broadcast unsubstantiated virus warnings from sources other than systems administrators.

(e) Broadcast e-mail messages to large groups of e-mail users (entire organizations) instead of targeting smaller populations.

(f) Employ for personal use applications using streaming data, audio, and video; malicious logic and virus development software, tools, files; unlicensed software; games; Web altering tools/software; and other software that may cause harm to Government computers and telecommunications systems.

g. Web blocking. Per AR 25-2 , the use of Web access blocking/filtering tools is authorized for permanently blocking user access to inappropriate Web sites associated with the prohibited areas itemized in f , above.

h. Administrative, criminal, and adverse actions. Unauthorized use or abuse of DOD and Army telecommunications systems, to include telephone, e-mail systems, or the Internet, may subject users to administrative, criminal, or other adverse action.

i. Use of employee-owned IT. Use of employee-owned assets IT hardware or software to process unclassified Army-related work off the Government work site must comply with the provisions of AR 25-2. Use of employee-owned IT hardware or software that connects to the network at the work site is prohibited.